A Technique of Hiding Secrete Text in Wave File

Ashraf Abu-Ein, PhD
Al-Balqa' applied university
Faculty of Engineering Technology
Amman – Jordan

Ziad A. A. Alqadi
Al-Balqa' Applied University
Faculty of Engineering Technology
Amman – Jordan

Jihad Nader, PhD
Al-Balqa' Applied University
Faculty of Engineering Technology
Amman – Jordan

ABSTRACT

Steganography is the art of hiding secret data within other information (such as wave file) that it cannot be detected, but only by its intended recipient. Embedding secret text in wave file is a difficult process. There are varying techniques for embedding information in wave files. In this research a new simple technique of hiding secret information using wave files were produced, regardless the simplicity this technique it will be accurate and high confident.

This paper features a new technique that suggests that the secrete text is encoded through the use position vector into wave file. The position vector (PV) is to be initialized randomly and to be kept confidential between the sender and the receiver. The security level of this technique will be high and it can be increased by encrypting the secrete text or/and encrypt the wave file including the text.

Keywords

Steganography, wave file parameters: PSNR and MSE, position vector, encryption, decryption, hacking.

1. INTRODUCTION

The technique of hiding information where only the sender and targeted receiver are aware of the hidden information existence is called Steganography. There are different kinds of Steganography including text, image, audio, video and protocol. This research will focus on wave Steganography that deal with only audio. It depends on encrypting text into wave file. [2],[3].

There are a lot of studies that have focused on Stegsnography and data encryption-decryption Nevertheless, it can be noted that only a small percentage of such studies have covered on the subject of secure hiding secrete data message. Thus, it can be noted that there is a need for a technique that focuses in data hiding which provides secure data transmission and accurate data receiving.

R. Kaur [4] applied the multilevel procedure in audio Stegsnography which entrenched three messages in audio file, in level 1 conceal message by making use of LSB (Least Significant Bit) technique, in level 2 conceal message 2 in audio file from level 1 applying parity bit coding method, in level 3 conceal message 3 in resulted audio file from level 3 applying frequency hopping spread spectrum coding technique and compute Peak Signal to noise ratio (PSNR) and Mean Squared Error (MSE) at every level and scheme the audio file figure at each level. K.U. Singh [5] highlighted various audio Stegsnography methods like temporal domain method and Transform Domain Technique (e.g., Discrete Wavelet transform, Spread Spectrum, Tone insertion and Phase coding) then compared between these methods from strength and weakness. F. A. Sabir [6] applied both of cryptography and Stegsnography methods then encoded text using DES (Data Encryption Standard) and concealed it in wav file using time and frequency domain technique followed by examining the cover audio file into its frequency elements through the use of Hear filter. He then computed the value of SNR (Signal to Noise Ratio) which affirmed that the concealing in frequency domain is ideal than concealing in time domain. T. Sandhya[7] suggested technique based on integration of audio Stegsnography and cryptography that is based on dual density double tree complex wavelet Transform with blowfish encryption. It implements most influential procedure in the initial level of security which is very intricate to disrupt. In the subsequent level, it applies a changed LSB procedure to encrypt the message into audio thus ensures superior security. Taruna[8] applied a keyless randomization that is provided to supplement undisclosed information in numerous and variable LSBs. Cover signal is transformed into binary format and then with the suggested algorithm, binary cover signal is categorized into blocks of size 8x8 that have 16 bits per sub block, and then examining each sub block's first two Most Significant Bits (MSBs) to establish how many LSBs will be applied during attachment of secret data bits. PSNR values indicate that there is no obvious variance between cover audio signal and stego audio signal. R. Valarmathi [9] applied most authoritative algorithm in the initial level of security, which is very intricate to break. In the succeeding level it applies a modified LSB procedure to encrypt the message into audio. This system enhances better security. A. Chadha [10] technique is dependent on LSB management and attachment of terminated noise as undisclosed key in the message. This technique is used in data concealing in images. For data concealing in audio, Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT) were all applied.

N. Kaul [11] found that an audio message can be entrenched in an image through the use of LSB technique as well as the wavelet conversion. To conceal a speech in an image is puzzling since the scope of speech is greater than the size of an image. Number of bits in 1kb of speech is almost equal to an image. Burate D. J [12], suggested a new method to conceal text in speech in an environment that has no noise. We chose to operate in the digital field and conceal the text information within speech signal using audio Stegsnography method. Indeed, proposed technique enhances the hiding data rate. It's better to reserve the uniqueness of the speech carrier by engaging an entrenching instead of a replacement operation on the undisclosed text. To intensify security, Stegsnography has to be combined with cryptography. Nevertheless, our technique does not use any of the cryptography methods as it applies coding approach.

2. THE PROPOSED TECHNIQUE

The proposed technique can be implemented in various versions:

Version A

Selecting this version of the proposed technique can be applied implementing the following steps:

Embedding the secrete text phase:

1) Get the wave file (X) and retrieve the file size (FS).
2) Get the secrete text message (M) and retrieve the message size (MS).
3) Generate a random position vector, which will indicates the position in wave file where to hide the secrete text as follows:

   PV=fix (rand(MS,1)*FS)

4) Save PV to be used by the receiver.
5) Save the contents of wave file indicated by PV into B array.
6) Insert the secret text character by character into the indicated positions of the wave file (XX) after converting each character to a fraction by dividing it with 255.

Here we must notice that MF, MS and PV are secrete data and it is difficult to hack them.

Extracting the secrete text phase:

1) Get the wave file (XX), B, and PV.
2) From XX retrieve the secret messages from the positions indicated by PV and multiply each element by 255.
3) Insert B into the wave file, in the positions indicated by PV to get the original wave file.

Version B

This version can be used if we want a higher security level and it can be done by encrypting the secret text before embedding phase and decrypting the text after extracting phase and the encryption-decryption is simple and it can be performed as follows:

Encryption phase:

1) Reshape the secret message into a square matrix.
2) Generate a random square matrix(secrete) to be used as a private key for encryption-decryption
3) Apply matrix multiplication to get the encrypted text.
4) Reshape the text into its original size.

Decryption phase:

After extracting the encrypted message from wave file Apply the following:

1) Reshape the encrypted secret text into square matrix.
2) Get the secrete text matrix by applying matrix multiplication of the encrypted message and the inverse of the private key.
3) Reshape the decrypted secrete text to the original size.

Version C

For more security we can encrypt-decrypt the wave file using the same methodology used in version B.

Version D

To achieve highest level of security we can use a combined method of versions B and C.

3. IMPLEMENTATION

Different MatLab codes were written and implemented to test the various versions of the proposed technique. The wave files were tested using wave file parameters mentioned in [1].

Here are the results of one example:

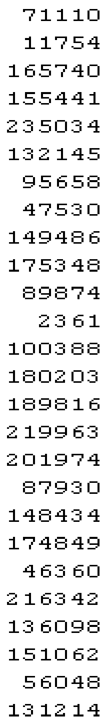
Secret text = this is my secrete message

Wave file: hawking02.wav

Wave file size = 239102

Secrete text size = 26

Position vector (PV) =



```
   71110
   11754
  165740
  155441
  235034
  132145
   95658
   47530
  149486
  175348
   89874
    2361
  100388
  180203
  189816
  219963
  201974
   87930
  148434
  174849
   46360
  216342
  136098
  151062
   56048
  131214
```

Figures 1, 2 and 3 shows the characteristics of the wave files during implementation:

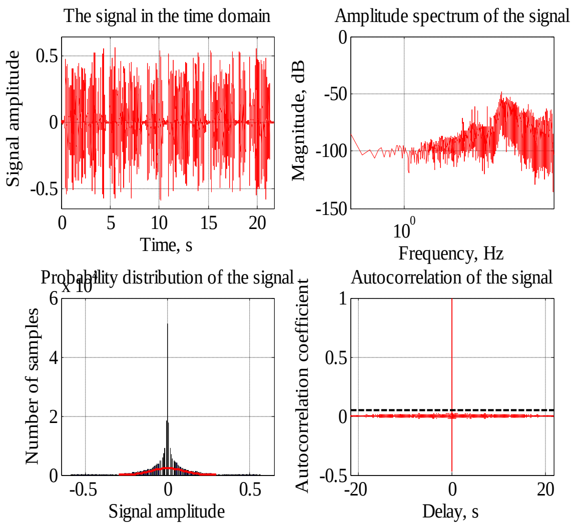


Figure 1: characteristics of original wave file

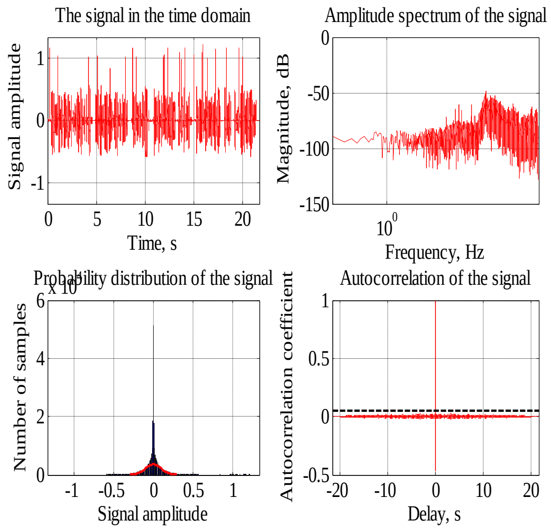


Figure 2: characteristics wave file after inserting the text

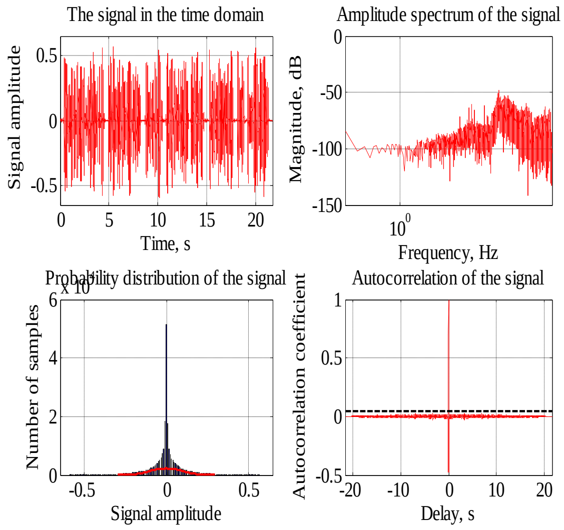


Figure 3: characteristics wave file after extracting the text

Table 1 shows the wave files parameters after executing the proposed technique:

Table 1: Wave files parameters

Parameter	**Original wave file**	**Wave file with secrete text**	**Wave file after extracting secret text**
Max value	0.5625	1.21	0.5625
Min value	-0.58594	-0.58594	-0.58594
Mean value	-0.00011629	-1.1674e-005	-0.00011629
RMS value	0.097825	0.098367	0.097825
Dynamic range D	37.1466 dB	43.7999 dB	37.1466 dB
Crest factor Q	15.1935 dB	21.7987 dB	15.1935 dB
Autocorrelation time	0.032744 s	0.032744 s	0.032744 s

From the obtained experimental results we can note the following:

- There is no damage of information in the wave file and the secret text.
- The security level is very high because position vector is confidential.
- We can increase the security level by adopting a suitable version of the technique.

Other versions of the proposed technique were implemented using different wave files and different secrete texts and the experimental results were acceptable and like those for the previous example.

4. RESULT

Using Matlab graphical user interface, the result can be obtain after compiling the program. In this technique the secret message can be hidden and regenerated in confidential position.

5. CONCLUSIONS

A new technique was introduced that have high level of security due to the confidential position of the vector. The proposed technique was very simple to implement while keeping the integrity of information. Many versions of this technique where introduced allowing for a various levels of security to be chosen from.

6. FUTURE SCOPE

The proposed method can be used with different kinds of Stegsnography such as image and video.

7. REFERENCES

[1] K. Matrouk, A. A. Hasanat and H. Alashalary, Prof.Ziad Al-Qadi and Prof. Hasan Al-Shalabi, "Speech fingerprint to identify isolated word person", World Appl. Sci. J., vol. 31, no. 10, pp. 1767-1771, 2014.

[2] Pushpa Aigal, Pramod Vasambekar, Hiding Data in Wave Files, International Conference in Recent Trends in Information Technology and Computer Science (ICRTITCS - 2012) Proceedings published in

International Journal of Computer Applications® (IJCA) (0975 – 8887).

[3] Adel A. Sewisy and others, Hidden Text into Audio Files, International Journal of Research Studies in Science, Engineering and Technology Volume 2, Issue 5, May 2015, PP 33-39 ISSN 2349-4751 (Print) & ISSN 2349-476X (Online)

[4] R. Kaur, Jagriti, H.Singh and R.Kumar, Multilevel Technique to improve PSNR and MSE in Audio Stegsnography. International Journal of Computer Applications, Vol.103, No.5, 1-4, (2014).

[5] K.U. Singh, A Survey on Audio Steganography Approaches. International Journal of Computer Applications, Vol.95, No.14, 7-14, (2014).

[6] F.A. Sabir, Hiding Encrypted Data in Audio Wave File. International Journal of Computer Applications, International Journal of Computer Applications, Vol.91, No.4, 6-9, (2014).

[7] T. Sandhya, A Novel Audio Steganography Scheme using Double Density lauD Tree Complex Wavelet Transform Secured with Modified Blow Fish Encryption. International Journal of Emerging Technology and Advanced Engineering, Vol.3, No.1, 63-72,(2014).

[8] Taruna and Dinesh, "Message Guided Random Audio Steganography using deifidoM LSB Technique", International Journal of Computers & Technology, Vol.86, No.7, 3464-3469, (2014).

[9] R. Valarmathi, M.SC. and M. Phil, A Novel Approach for Autography- AnoitanibmoC of Audio Steganography and Cryptography. International Journal of Emerging Technology and Advanced Engineering, Vol.4, No.1, 55-61, (2014).

[10] A. Chadha, N. Satam and R .Sood, An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution. International Journal of Computer Applications, Vol.77, No. 13, 37-45, (2013).

[11] N. Kaul and N. Bajaj, Audio in Image Steganography based on Wavelet Transform. International Journal of Computer Applications, Vol.79, .oN 3,7-10,(2013).

[12] Burate D. J, Performance Improving LSB Audio Steganography Technique. , Vol.4, No.1, 67-75, (2013).